Configuring Structural Authorizations

Cheat Sheet

Pre-Structural Authorization Questions

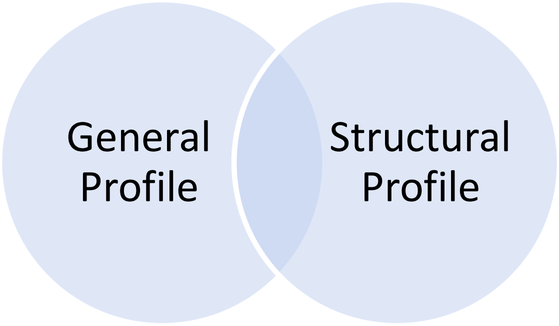
Before implementing structural authorizations, ask and answer the following questions:

- What types of HR functions are performed in my organization (i.e. – payroll, manager, trainer, etc.)?
- What types of profiles do these functions require in order to operate correctly (i.e. – profiles = who access can be performed on)?
- Is there anyone in my company performing more than one of these functions?
  - Context-sensitive question – if you answer yes, you must consider context approach to structural authorizations.

Understand the Basics – Profile Concept (Who vs. What)

Structural authorizations give access to a user based on an overall profile, which is the combination of General Profiles and Structural Profiles.

- General Profiles – Determine which object data (infotype/subtype) and which type of authorization (read/write) a user has for objects in their profile.
  - **The What**
- Structural Profiles – Subsets of your organizational structure that determine which objects in the structure a user has access to.
  - **The Who**



Note - The intersection of the profiles is the access granted to a user.

Context Solution

Context issues arise when you have users performing more than one role in your organization, requiring accessibility to different groups for different purposes.

- P_ORGIN replaced by P_ORGINCON/P_ORGINXXCON.
  - Only difference in authorization objects is the addition of a new authorization field (PROFL) to assign structural profiles to particular authorization objects.
  - Only available for P_ORGIN authorization objects/infotypes, not PLOG.

Analyzing Your HR Authorization Settings

SAP provides a nice tool that you should utilize during your structural authorizations implementation and beyond that allows you to quickly analyze HR authorization information settings in your system.

Transaction: HRAUTH

The Overview tab allows you to view information on authorization switch settings, authorization related BADIs, structural profiles and user assignments, indexing programs and jobs, etc.

The User-Specific tab allows you to view authorization information for specific users, including assigned roles, structural profiles, indexing entries, etc.

Structural Authorization Switches

Transaction: OOAC
Table: T77S0

Switch	Description
AUTSW / ORGPD	Main switch for activating structural authorizations
AUTSW / INCON (Context)	Switch for context-sensitive structural authorizations (P_ORGINCON)
AUTSW / XXCON (Extended Context Check)	Switch for extended context-sensitive structural authorizations (P_ORGINXXCON)
AUTSW / NNCON (Customer Context)	Switch for customer-specific context-sensitive structural authorizations (P_NNNNCON)
AUTSW / DFCON (Default Position)	Controls how system reacts to personnel numbers not linked in org structure in context solution (persons on default position)
AUTSW / ADAYS	Tolerance time for authorization check specifying the length of time, in case of org change, that user has access to data he/she created for a person. (not applicable in context solution)

Maintaining Structural Profiles

Transaction: OOSP
Table: T77PR

Field	Description
Auth. Profile	Defined name of authorization profile
No.	Sequence number of elements of authorization profile. A profile can contain many elements of various root objects and supporting values.
Plan Vers.	Key of the plan version for objects in profile element.
Obj. Type	Object type of root object
Object ID	Root object ID. Can be defined directly or left blank and supplied by function module. Evaluation path for element runs off of this root object.
Maint.	Flag for function codes in Personnel Management defined as ‘maintaining’ and ‘non-maintaining’. If processing type *Maintenance* is flagged in table T77PR for a profile, it means that function codes classed as "maintaining"

Field	Description
	in table T77FC can also be executed for the authorized objects.
Eval Path	Evaluation path to be used with respect to root object. Objects are evaluated by the evaluation path and returned as part of the profile.
Status Vector	List of one or more statuses for Relationship infotypes. Used to identify the status that a Relationship infotype must have in order for an object to be reported on.
Depth	Depth of organization structure evaluated by structural profile.
Sign	A +/- sign used if structural authorization profiles are to be created that are to process the structure "from top to bottom".
Period	Validity period for restriction of structure in structural profile.
Function Module	Optional function module that can be used to dynamically determine root object of element in structural profile.

Importance of Evaluation Paths

Transaction: OOAW

Evaluation paths are the most important element of a structural profile, along with the root object. Without evaluation paths, structural profiles would only grant access to defined root objects.

Function Modules for Root Objects

The use of function modules in structural profiles allow for dynamic root objects to be defined for a profile depending on a user. Standard SAP function modules are provided below, custom function modules can be written for any purpose.

Function Module	Description
RH_GET_MANAGER_ASSIGNMENT	Finds the root organizational unit with which the user is related via the A012 (manages) relationship
RH_GET_ORG_ASSIGNMENT	Finds the root organizational unit to which the user is assigned

User Profile Assignment and Review

Transaction: OOSB
Table: T77UA

Structural profile assignments can be viewed/maintained here. Clicking the blue Info button allows you to view all objects returned for a user/profile assignment.

Steps for Indexing

If system performance suffers from structural authorizations, especially the context approach, indexing can be utilized to improve performance by indexing users with large numbers of objects in their structural profiles. Steps for successful indexing are as follows:

1. Run program RHBAUS02 to analyze user population and place a certain level of assigned objects in table T77UU.
2. Run program RHBAUS00 to index users in table T77UU (can be run for entire population of table or specific individuals).

3. Run program RHBAUS01 periodically to clean-up previously indexed users that are no longer in table T77UU.

Indexing must run frequently as changes in the org structure will not be reflected in user access until indexing occurs (nightly run recommended, during low system usage period).

Position-Based Security Know-How

Position-based security involves the assignment of security roles to org objects such as jobs, positions, or org units. The security role assignments can then be inherited to users based on the org structure automatically, reducing security administration time.

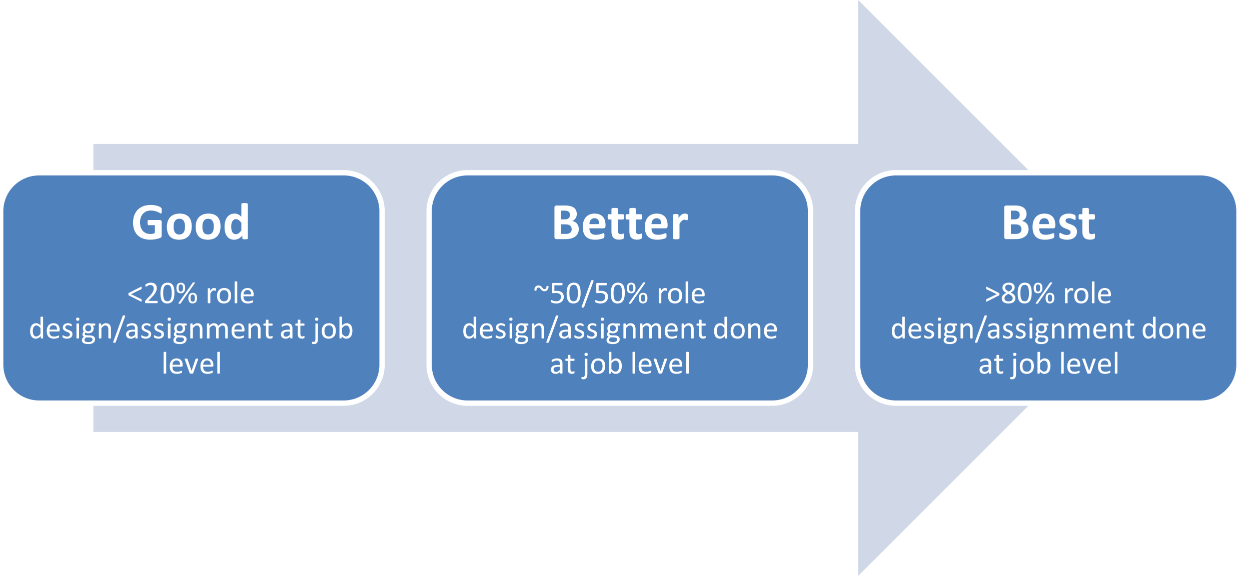
The table below highlights key information for the management of position-based security.

- Role assignments can be made via the Relationship infotype (1001), subtype B007 (Is described by) from a Job (C), Position (S), or Org Unit (O), to a Role (AG).
- Running the *User Master Data Reconciliation* program (t-code PFUD) with the ‘HR Organizational Management: Reconciliation’ option will evaluate these indirect role assignments to the appropriate user IDs and automatically assign authorizations accordingly.

Position-Based Security Know-How

Remember the following when designing position-based security:

- Analyze your job catalog first
  - Are your jobs effectively setup where all employees in one job need consistent system access?
- Ask yourself what each job in your company requires for system access
  - Use job descriptions as a guide
- Define security at job-level as much as possible
- Identify what jobs/positions require security roles
- Evaluate effectiveness of position-based security design using the following:


Good
<20% role design/assignment at job level
Better
~50/50% role design/assignment done at job level
Best
>80% role design/assignment done at job level